Defining critical technologies for special operations

McLaughlin, Lawrence W.

Monterey, California. Naval Postgraduate School

NAVAL POSTGRADUATE SCHOOL
Monterey, California

THESIS

DEFINING CRITICAL TECHNOLOGIES FOR SPECIAL OPERATIONS

by

Lawrence W. McLaughlin

December 1999

Thesis Advisor:	Gordon McCormick
Co-Advisor:	Anna Simons

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. AGENCY USE ONLY *(Leave blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	December 1999	Master's Thesis

4. TITLE AND SUBTITLE
Defining Critical Technologies for Special Operations

5. FUNDING NUMBERS

6. AUTHOR(S) McLaughlin, Lawrence W.

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Naval Postgraduate School
Monterey, CA 93943-5000

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)

10. SPONSORING / MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES
The views expressed in this thesis are those of the author and do not reflect the official policy or position of the Department of Defense or the U.S. Government.

12a. DISTRIBUTION / AVAILABILITY STATEMENT
Approved for public release; distribution is unlimited.

12b. DISTRIBUTION CODE

13. ABSTRACT ***(maximum 200 words)***

As the military forces of the United States continue to draw down, Special Operations Forces (SOF) are playing a greater role across the entire spectrum of conflict. In order to maintain its relative advantage, SOF is using technology as a means to leverage limited resources – sometimes to the point that mission accomplishment depends critically on a technology's availability. Adversaries will attempt to challenge our advantages. Whether Special Operations Forces are prepared to operate in a degraded environment could determine success or failure.

This thesis examines the issue of *critical* technologies in special operations. *Critical* technologies are defined according to three variables – level of dependence, degree of vulnerability, and substitutability. By examining technologies against these three variables, SOF can gain a better understanding of the impact to SOF operations if a technical capability is lost. Three technologies are examined to illustrate the model – the use of Radar in the Battle of Britain, the Global Positioning System, and UHF Satellite Communications.

By applying the model to actual cases, I hope to encourage SOF decision-makers to closely examine our growing reliance on vulnerable technologies as a force multiplier and provide recommendations to prevent undue reliance on those technologies.

14. SUBJECT TERMS
Technology, Special Operations, Global Positioning System, Satellite Communications

15. NUMBER OF PAGES
104

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFI- CATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL

NSN 7540-01-280-5500

Standard Form 298 (Rev. 2-89)
Prescribed by ANSI Std. 239-18

THIS PAGE INTENTIONALLY LEFT BLANK

Approved for public release; distribution is unlimited

DEFINING CRITICAL TECHNOLOGIES FOR SPECIAL OPERATIONS

Lawrence W. McLaughlin
Major, United States Air Force
B.S., United States Air Force Academy, 1988

Submitted in partial fulfillment
of the requirements for the degree of

MASTER OF SCIENCE IN DEFENSE ANALYSIS

from the

NAVAL POSTGRADUATE SCHOOL
December 1999

ABSTRACT

As the military forces of the United States continue to draw down, Special Operations Forces (SOF) are playing a greater role across the entire spectrum of conflict. In order to maintain its relative advantage, SOF is using technology as a means to leverage limited resources - sometimes to the point that mission accomplishment depends critically on a technology's availability. Adversaries will attempt to challenge our advantages. Whether Special Operations Forces are prepared to operate in a degraded environment could determine success or failure.

This thesis examines the issue of *critical* technologies in special operations. *Critical* technologies are defined according to three variables - level of dependence, degree of vulnerability, and substitutability. By examining technologies against these three variables, SOF can gain a better understanding of the impact to SOF operations if a technical capability is lost. Three technologies are examined to illustrate the model - the use of Radar in the Battle of Britain, the Global Positioning System, and UHF Satellite Communications.

By applying the model to actual cases, I hope to encourage SOF decision-makers to closely examine our growing reliance on vulnerable technologies as a force multiplier

and provide recommendations to prevent undue reliance on those technologies.

TABLE OF CONTENTS

I. INTRODUCTION 1

A. BACKGROUND 1

B. RELEVENCE 2

C. PURPOSE 3

D. DEFINING CRITICAL TECHNOLOGIES 4

1. Dependence 5

2. Vulnerability 7

3. Substitutability 8

E. CASE SELECTION 10

II. THE BATTLE OF BRITAIN 13

A. INTRODUCTION 13

B. BACKGROUND 14

1. The Prefight Numbers 16

2. The Chain-Home System 18

C. RADAR AS A *CRITICAL* TECHNOLOGY 20

1. Dependence 21

2. Vulnerability 22

3. Substitutability 24

D. SUMMARY 25

III. GLOBAL POSITIONING SYSTEM 27

A. INTRODUCTION 27

B. BACKGROUND 30

1. GPS Segments 30

2.GPS Signal 32
C.GPS AS A CRITICAL TECHNOLOGY 35
1.Dependence 36
2.Vulnerability 40
3.Substitutability 49
D.SUMMARY 52
IV. SATELLITE COMMUNICATIONS 55
A.INTRODUCTION 55
B.BACKGROUND 58
1.Satellite Operation and Components 59
2.Frequency Bands 60
3.Orbits 61
C.SATELLITE COMMUNICATIONS AS A CRITICAL TECHNOLOGY 64
1.Dependence 65
2.Vulnerability 68
3.Substitutability 70
D.SUMMARY 74
V. SUMMARY/ FINDINGS/ RECOMMENDATONS 77
A.SUMMARY 77
B.FINDINGS 79
1.Electro-magnetic Pulse 81
C.RECOMMENDATIONS 85
LIST OF REFERENCES 89
INITIAL DISTRIBUTION LIST 93

I. INTRODUCTION

A. BACKGROUND

Technological advancement is a critical aspect of any study of military operations. It is impossible to dissociate war from the technological means of fighting war. John H. Morse, former US Assistant Secretary of Defense, stated, "It is more the march of technology than it is the political decisions which drives the nature and structure of our societies, our strategy, the nature of military forces, their structure and the doctrine they develop" (Holmes, 1988, p. 7). Technology, in short, has played a central role in shaping the strategy, doctrine, and organization of military units. The longbow, repeating rifle, maxim machine gun, airplane, tank, radar, and radio have all had a major impact on how war has been conducted throughout the ages.

Although technology has played a vital role, it has significant limitations. Adversaries have been very successful in countering technological advancements and "leveling the playing field". The Zulus against the British, the plains Indians against General Custer, the Vietnamese against the French and Americans, the Afghans against the Soviets- all examples of a less sophisticated foe defeating a technologically superior force.

B. RELEVENCE

> More than ever SOF will depend on leading-edge technology to provide the critical advantage and to support participation in a growing number of technologically complex and challenging missions and operations. (*SOF Posture Statement*, 1998, p. 40)

> Technological superiority enables small, highly trained teams or individuals to successfully accomplish tasks that would be too costly or physically impossible for larger forces. (*SOF Posture Statement*, 1998, p. 11)

Special Operations Forces (SOF) play a unique role as a strategic asset of the United States. The changing world dynamics have placed SOF in a precarious position. As the military forces of the United States continue to draw down, SOF is playing a greater role across the entire spectrum of conflict. Our forces are continuously using technology as a means to leverage limited resources and USSOCOM is especially committed to the development of new technologies to maintain a relative advantage. Conversely, SOF must be careful not to put too much emphasis on technologies that could be countered by enemy action. With the proliferation of advanced technologies in an ever-shrinking world, it is likely that future adversaries will develop measures to counter our advantages. We must not forget that combat is a dynamic interaction between two opposing forces, therefore,

an advantage in capability at the beginning of a conflict may be degraded or eliminated. Whether SOF is prepared to operate in a degraded environment may be critical to determining success or failure. As the previous excerpts from the SOF Posture Statement imply, there is every indication that SOF will continue to pursue more advanced technologies to maintain an 'edge'. It is therefore essential to step back and examine how new technologies are being used, the effect of their possible loss, and develop a means to examine when a technology becomes so important that mission accomplishment rests on its availability.

C. PURPOSE

The purpose of this research is to answer the following questions:

- How can we determine which technologies are *critical* to Special Operations Forces?
- What are the vulnerabilities of these technologies?
- What is the potential impact on SOF if these technologies are lost?

This thesis will develop a model that can be used to identify technologies that are essential to SOF operations and consider the impact of the loss of these technologies on mission accomplishment. An additional purpose of this

effort is to encourage SOF decision-makers to closely examine our growing reliance on technology as a force multiplier. It should encourage commanders and operators to look beyond the initial engagement and develop a longer term view of warfare against an adversary with the means to eliminate or significantly degrade our technological advantage. The first step in this process is to define what makes a technology *critical*. The following section defines critical technologies based on three important variables.

D. DEFINING CRITICAL TECHNOLOGIES

The idea of critical technologies is not new to the Department of Defense. For over a decade, the DoD has been required to submit to Congress a list of technologies that it considers "critical to ensuring the continued qualitative superiority of US weapons systems" (Jefferson, 1989). The technologies that appear on this list are not specific to any service or mission and are often very general. Some of these technologies include microelectronics, robotics, integrated optics, data fusion, and lightweight composite materials.

The main purpose of the list is to identify those technologies that are critical to maintaining capabilities in the future and defining those areas that require

coordination and focus of research and development efforts (Walsh, 1997). This is where my analysis differs from the traditional view. Instead of looking at what capabilities will be critical in the future, this study looks at what technological capabilities Special Operations Forces have *now* that are necessary to their success.

The first step in defining *critical* technologies for Special Operations Forces is to clearly specify what makes a technology "critical". Three factors will be used to determine criticality. The first factor is *dependence*. The second factor is *vulnerability*. The last factor deals with the *substitutability* of the technology in question. The remainder of this section will discuss the three criteria in detail and how the criteria can be used to evaluate selected technologies.

1. Dependence

The first factor in defining critical technologies for SOF is *dependence*. To be considered critical, the technology must be *required* to effectively perform a mission tasking. The task may be as broad as one of the SOF principal missions or as narrow as a Mission Essential Task List (METL) item, as long as the METL item is essential to the completion of the operation. Considering that much of the technological advancements in weapon systems,

communication systems, navigation systems, and delivery systems are rather new to SOF, dependency on a technology has a broader meaning than initially realized. It is obvious that if a mission cannot be performed without a specific technology then the dependency requirement is satisfied. The condition of dependency can also be satisfied if the mission can be accomplished in the absence of the technology, but much less effectively and at a much higher risk.

Dependency, in this case, will vary by degree. For example, a SF team is tasked to conduct a special reconnaissance (SR) mission lasting an extended period of time. The mission is to provide daily reports on the mobilization of enemy forces. To effectively carry out this mission, secure long-range communications -- the relevant technology -- are required. Although alternate (nonsecure) methods of communications may be available, the risk of team compromise or mission failure significantly increases with their use. This example illustrates an important point. Although the recon mission can still be accomplished using a sub-optimal technology, the condition of dependence on a *critical* technology is still satisfied.

As we will see in the next chapter, the British were very dependent on RADAR to warn of German attacks during the

Battle of Britain. Could the British have won the Battle of Britain without RADAR? Possibly, but they would have been much less effective and would have sustained much greater losses.

2. Vulnerability

The second determinate of criticality is *vulnerability*. To be vulnerable means to be susceptible to attack. SOF exploits a variety of technologies to gain a relative advantage over an adversary. If we view war as a series of engagements between two competent adversaries, it is obvious that if one side has a relative advantage then the other side will attempt to counter that advantage through whatever means available. Therefore, SOF must be aware that the enemy may be in a position to significantly degrade whatever technological advantage U.S. special operations forces may enjoy during the initial phase of the conflict.

Some technologies, of course, are more susceptible than others are. Re-breathers used by Navy SEALs are an essential technical item. They provide the SEALS with an important capability necessary to complete a variety of combat tasks. Being a completely self-contained and passive system, the re-breather is virtually invulnerable to enemy countermeasures. The same is true of night vision devices. Although very important to conducting night operations,

night vision devices cannot be targeted (and, hence, degraded) in a comprehensive manner. Each device must be targeted individually - an almost impossible task. Conversely, the enemy can disrupt the use of the electromagnetic spectrum in a variety of ways. Therefore, for the purpose of this study, re-breathers and night vision devices are not considered as critical technologies. Radio communications, by contrast, are potentially vulnerable and could be considered critical if they meet the other criteria. For a technology to be vulnerable, it must have an exploitable weakness, either initially or over the duration of an extended conflict.

3. Substitutability

The final criterion we will use to define a critical technology is *substitutability*. Special Operations Forces may be dependent on a technology that is vulnerable to enemy action, but that technology is not considered critical if a ready substitute is available resulting in little or no loss of capability. Substitutability is closely related to dependence, but they are distinct criteria. SOF is always searching for leading-edge technologies to sustain an advantage. Often new technologies are incorporated into SOF operations as a supplement to, not a replacement for, existing equipment. For example, computer-based flight

planning systems are provided to all SOF aircrew. These systems can reduce the amount of time required to plan a mission and produce excellent mission aids. Although it may take slightly longer; a map, pencil, plotter, and compass could produce a near equivalent product. In general, actual mission accomplishment may not be strongly affected by the method used to plan a flight. For a technology to be designated as critical, it must provide a unique advantage that cannot easily be duplicated through other means or technologies.

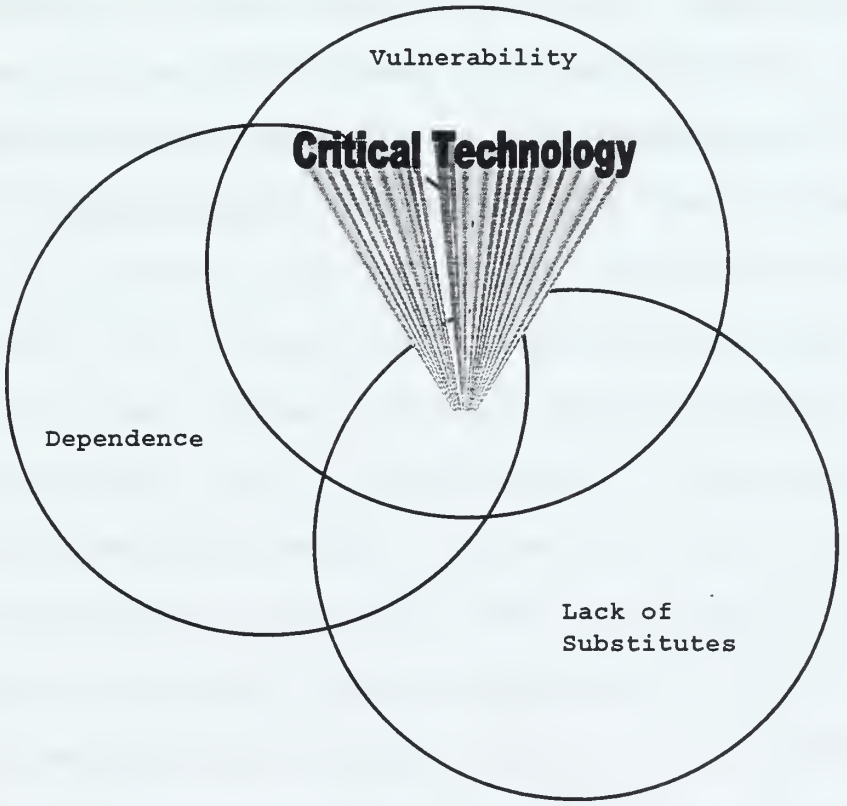

Figure 1. The Criteria of "Critical Technologies"

E. CASE SELECTION

The degree of *dependence*, *vulnerability*, and *substitutability* that characterize a technology can change based upon how the technology is used, what mission it is used for, and who uses it. SOF currently has nine principal missions and eight collateral activities, all of which can involve numerous tasks that are essential to mission success. A technology deemed critical to counterproliferation might not be considered critical for conducting special reconnaissance. It is clearly not possible in this study to analyze every technology in relation to every SOF mission task. The goal is rather to select a technology sample that can be used to illustrate the problem of technological "criticality". By concentrating on technologies that have applications across a broad range of missions and SOF units, it will be easier to apply lessons learned to more specific cases of single missions or tasks. In addition to the historical case presented in the next chapter, I have selected the Global Positioning System and UHF Satellite Communications as possible *critical* technologies for SOF. Obviously, these two technologies are not the only possible technologies *critical* for SOF, but they are current examples that illustrate the

qualities of dependence, vulnerability, and substitutability as they apply to SOF operations today.

The following chapter includes an historical analysis of the Battle of Britain and the role radar played in its successful outcome. Radar was the backbone of the British air defense system and a *critical* technology for the British. The British air defense system provided the British with a relative advantage over the superior German Air Force, but it was a fragile advantage. Even though vulnerable to enemy attack, radar was the only technology available to provide the British with adequate warning of German attacks. The three criteria of critical technologies - dependence, vulnerability, and substitutability - are presented in the following important historical example.

II. THE BATTLE OF BRITAIN

A. INTRODUCTION

It is undisputed that advances in technology have played an essential role in the conduct of conflict throughout the ages. There are obviously countless technological advancements, some mentioned in the previous chapter, that have shaped war and changed history in the process, but there is one technological advancement that is often overlooked - Radio Detection and Ranging, more commonly known as Radar. Some form of radar is used in almost every major weapon system, from airplanes, to ships, to range finders on individual tanks. David Fisher (1988), author of *A Race on the Edge of Time: Radar - The Decisive Weapon of World War II*, states, "Taken all in all, radar must be the most important scientific/ political/ military invention of them all, bar none" (p. xi). Although this statement may be contested, it is clear that radar has played a significant role in warfare.

Radar was first used by the British during World War II to detect German aircraft approaching England. The early warning of German attacks provided by the British radar system proved essential to preventing the German invasion of England. An examination of the use of radar before and

during the Battle of Britain provides an excellent example of a *critical* technology. The three criteria of dependence, vulnerability, and substitutability are clearly demonstrated by this well documented case.

B. BACKGROUND

In just two short years, Hitler's Germany had gained control of most of the European continent. Czechoslovakia, Austria, Poland, Belgium, Holland, and France were all under German control. The British Expeditionary Force (BEF), along with over 100,000 French troops were isolated around the port of Dunkirk on the Franco-Belgian border (Clark, 1966). Under immense German pressure, the BEF and French forces were forced to flee across the English Channel, relinquishing the last stronghold on the continent. With the signing of the Treaty of Non-aggression between Germany and Russia, only one country remained successfully at war with Germany - Great Britain. Realizing that Britain would not come to terms like the French, "the invasion and subjugation of Britain therefore became essential to the Germans" (Clark, 1966, p. 23).

Both the British and the Germans learned valuable lessons during Hitler's campaigns of 1939 and 1940. One very important lesson was the value of airpower. The rapid

and overwhelming success of German ground operations relied heavily on the Luftwaffe's support for advancing ground forces. German bombers were very effectively employed as long range artillery in direct support of the army. However, in order for the bombers to successfully conduct attacks in daylight they had to be protected by fighter escorts (Clark, 1966). Air superiority became a necessary condition for a ground campaign - a point clearly demonstrated at Dunkirk.

The rescue of the BEF and French forces at Dunkirk relied on a number of things, one of which was the lack of German air superiority over the Dunkirk beaches (Clark, 1966). Allied planes flying out of France and England were able to effectively engage the Luftwaffe, slow the German ground offensive, and allow retreating British and French forces to cross the channel to England in everything from fishing boats to private yachts.

The Germans knew that in order to successfully cross the channel and conduct an invasion of England, command of the air had to be achieved. "All that remained to be done before the great venture started was to gain control of the air. Without that, as the Germans well knew, they were unlikely to get ashore, let alone stay there" (Clark, 1966, p. 131). For *Operation Sea Lion* (the code name assigned to

the German plan to invade England) to commence, the Luftwaffe had to neutralize British Fighter Command.

Fighter Command was a formidable force. Developed over nearly two decades, Fighter Command was well organized and committed solely to the defense of England. However, defeating the German Luftwaffe would not be an easy task. The "Battle of Britain", whose outcome would determine the future course of WW II, was fought with Germany's Luftwaffe having a distinct numerical advantage over Britain's Fighter Command.

1. The Prefight Numbers

By the summer of 1940 -- the start of the Battle of Britain -- the British were outnumbered in frontline aircraft two to one. The Royal Air Force (RAF) had approximately 2900 aircraft of all types, the Luftwaffe over 4,500 (Posen, 1984); hardly the best of odds for a nation now isolated from the European continent and fighting solo against the formidable German war machine. Looking more closely at the numbers reveals a clearer, yet darker picture.

"Single-engine, single-seat fighters were the key element of both forces" (Posen, 1984, p. 94). The fighters were the aircraft that determined which side had command of the air. Without command of the skies, bombers were much

less effective and ground forces were susceptible to attack from enemy aircraft. Throughout the battle, Britain was able to close the gap, especially in fighters, but never approached a numerical advantage. Even at the peak of RAF size, between 550 and 650 British Hurricanes and Spitfires faced some 1,700 German fighters and bombers (Posen).

The qualitative difference was not nearly as great as the quantitative difference between the Luftwaffe and RAF. In fact, the Luftwaffe and RAF planes were quite evenly matched (Mosley, 1977). The British Spitfire and German Bf 109 were the best aircraft and their performance capabilities were very similar. British Hurricanes were a bit inferior and the Bf 110s were the worst. Even with somewhat evenly matched aircraft, the overall qualitative advantage was still with the Germans. The number of Spitfires seldom was over 250 and usually closer to only 200. The Germans had over 600 Bf 109s (Posen, 1984). Quality and quantity of aircraft was not the only issue facing the RAF at the start of the Battle of Britain.

The RAF was also plagued with a shortage of pilots. The British lost nearly 300 pilots over France and Belgium in just the few weeks of war on the continent (Clark, 1966). Most of the men lost were experienced aviators. In contrast, the Germans had a large pool of experienced

pilots, combat tested over Poland and Western Europe. The British could only effectively train sixty-five pilots a month, sometimes not keeping up with combat losses (Clark). Luckily, since the Battle of Britain was almost exclusively fought over England, RAF pilots could parachute or crash-land on friendly soil enabling them to be back in action rather quickly. This proved essential to maintaining enough experienced pilots to fly the planes (Mosley, 1977). Yet, there must have been some further reason why the British were able to overcome the Germans' qualitative and quantitative advantages. The answer is radar.

2. The Chain-Home System

> Early warning was one of the most important keys to victory. Without it the quality of the machines, the training of the pilots, or the courage with which they fought against such heavy odds would hardly have availed. (Clark, 1966, p. 116)

The British knew that their country was becoming increasingly vulnerable as aircraft cruise speeds tripled and bombing capabilities increased at an exponential rate. No longer could the British rely solely on visual warning to prepare for an impending attack. The idea that an aircraft could be detected by using radio waves had not even been thought of just five years before radar's decisive use against the Germans in 1940. The development of radar in

such a short period of time is an indication of the ingenuity of key individuals in the British scientific community. One such individual is Watson Watt - generally regarded as the father of radar (Fisher, 1988). Watt was the first to suggest that radio beams could be used to detect aircraft and was instrumental in designing and building the extensive radar system that spanned the entire east and south coast of England. The technology of radar was vital to the British, but was only one part of a much larger system that made up the air defense network.

The protection of England depended on an intricate web of radio towers, receiver stations and control centers. Twenty-one radio towers and control centers were established to maintain unbroken coverage along the entire coast. Each control center was directly linked to a single Fighter Command "Filter" center that consolidated the information and resolved any discrepancies in center reporting. The Filter center then passed the information on to the Group Headquarters which allocated the targets and controlled the intercepts with the aid of the control centers at each "Chain Home" site (Posen, 1984). The Chain Home system could detect aircraft over 100 miles out and even determine the relative size of the German formations giving Fighter Command the ability to scramble the proper number of fighter

squadrons to intercept the intruders. The controllers could even determine aircraft elevation. Altitude indications, however, were still much less reliable than azimuth and distance information (Fisher, 1988).

C. RADAR AS A *CRITICAL* TECHNOLOGY

The Luftwaffe had to obtain command of the air over the channel and along the coastal regions of England to execute a successful landing during *Operation Sea Lion.* The only thing that could prevent German command of the air was Fighter Command, therefore, the survival of Fighter Command was paramount for the British. After evaluating radar against the three criteria of critical technologies - dependence, vulnerability, and substitutability - it is easy to see how important radar was to Britain's success. Radar was *critical* to Fighter Command's, and hence, Britain's survival.

1. Dependence

> Fighter Command knew an invasion loomed but did not have the fuel or planes to maintain the standing patrols in anticipation of enemy raids. Nor did the country have the time to breed another crop of brave and intelligent young men if German bombers surprised planes and pilots on the ground. The nation's best hope for hanging on rested on being able to spot the Luftwaffe far out over the English Channel and then deploying its thin resources to meet the threat at hand. On this vital front, everything depended on the Chain Home radar network. (Buderi, 1996, p. 89)

The above quote from Robert Buderi in, *The Invention that Changed the World*, summarizes why the British were so dependent on radar. England, at the nearest point, was only twenty-two miles from German controlled territory. Launched from bases on the coast of France and Belgium and travelling over 250 mph, German aircraft could be over the southwest coast of England in minutes. The British were outnumbered and suffered from a shortage of pilots. It was not possible to continuously have enough aircraft airborne to counter a German attack, nor were there enough pilots to maintain the very short alert response times required if the British had to rely on visual sighting of German aircraft crossing the coast.

The RAF could ill afforded to allow the Germans to surprise them and destroy the aircraft on the ground. The only way Fighter Command could both fight and survive was to

husband their resources and engage the Germans only on terms favorable to the British. The British depended on radar to provide adequate warning of German intentions so that the *minimum* number of aircraft could be launched from the *right* airfields at the *right* time. Due to limited fuel reserves, an early launch could be just as disastrous as a late launch. Only with radar were the controllers on the ground able to place the defending squadrons where they could do the most good (Clark, 1966).

2. Vulnerability

The twenty-one Chain Home stations on which the British depended were quite vulnerable to enemy attack. Each station consisted of a tall metal or wooden antenna tower, a control center that housed the radarscopes, and the living quarters of the radar operators. The German targeted the towers but found them very difficult to hit due to their size and construction (Clark, 1966). The achillies heel of the stations was the control centers and living quarters.

The highly trained personnel manning the stations, so essential to its operation, were largely unprotected from enemy attack. The work centers and quarters were often flimsy wooden huts, hastily camouflaged, yet still easily visible to enemy bombers (Mosley, 1977). Luckily, the Germans did not realize the importance of the buildings

surrounding the towers and never mounted a significant campaign against them. Stations were hit periodically and taken out of action, but the Germans never effectively exploited the subsequent gaps in the radar coverage.

Toward the end of the Battle of Britain, the Germans did try to minimize the advantages of British radar by altering their tactics. The Luftwaffe would precede their bomber attacks with large fighter sweeps near the French coast in an attempt to confuse the radar operators and force the British fighters to launch unnecessarily. Numerous feint attacks would be followed by the main attack, with the goal of catching the British squadrons off balance and low on fuel (Clark, 1966). Using these tactics, the Germans began to inflict heavier losses on Fighter Command. Fortunately for the Allies, these tactics were developed too late in the campaign to affect the outcome.

The survival and continued effectiveness of the British radar system was not due to its invulnerability. The entire system was actually quite vulnerable and was successfully attacked, although often by accident. Radar's continued existence had much to do with a German intelligence failure. The Germans could never obtain enough information to find the radar system's physical weaknesses and did not develop

the tactics necessary to defeat the radar system's operational weaknesses until it was too late.

3. Substitutability

Substitutability is the final criterion that defines radar as a *critical* technology for the British in the Battle of Britain. It is clear that early warning of German operations was absolutely essential to the outnumbered RAF to succeed. It was a critical force multiplier. Although other methods of detection were attempted, radar was the only technology available at the time that could provide the advantage required to keep Fighter Command in the game. Although radar did prove successful, using radio waves to detect aircraft was not the only method the British tried. Sound detection was the first method tried to warn of approaching aircraft.

The first attempt to detect aircraft at long ranges was with sound waves. The key to the system was an acoustically molded wall 200 feet long and 25 feet wide. Imbedded in the wall were numerous extremely sensitive microphones. It was envisioned that a vast system of directional microphones would detect airplanes far before the airplane came into view (Fisher, 1988). The tests proved to be a failure. The scientists found that any extraneous noise affected the accuracy of the devices.

Another problem was with the physics of sound. Considering that sound travels at only 700 miles per hour (only about twice the speed of the bombers), by the time the sound reflected from the plane and was received by the microphones, the aircraft were no longer where the sound detectors indicated (Fisher).

An obvious solution was airborne surveillance to detect the launch and formation of German air elements over the continent. This tactic, however, was also out of the question. First, the RAF did not have the manpower or equipment to support continual surveillance. Second, it would be very hard for the airborne surveillance aircraft to effectively cover all the possible German airbases because they would have to maintain visual contact with each one. Lastly, surveillance aircraft would have been very vulnerable to German fighters over the enemy bases. It is clear that radar was the only effective means to provide the required warning so essential to Britain's eventual success in stopping the invasion of England. There was no effective substitute.

D. SUMMARY

The summer of 1940 was a desperate time for the British. The Germans controlled much of the coast of

Western Europe and were preparing for the invasion of England. In order to ensure a successful channel crossing the Germans had to have command of the air. The only thing that stood in Germany's path was Great Britain's Fighter Command. Considering the Germans' qualitative and quantitative advantages, the defeat of Fighter Command should have been no problem for the experienced Luftwaffe.

Radar, a *critical* technology for the British, allowed an out-gunned and out-numbered force to achieve a *relative* advantage and ultimately succeed against the German onslaught. Radar easily satisfies the three criteria outlined in the previous chapter. The British depended on radar to warn of German bombing raids enabling Fighter Command to selectively launch only those squadrons necessary to meet the approaching threat and protect their aircraft from being attacked while on the ground. Only with radar could the British husband their scarce resources and survive through the summer. Although not fully exploited by the Germans, radar was quite vulnerable by direct attack of the control centers and by tactical deception. Lastly, radar was the only thing available that could give the British the advantage they needed to survive the Battle of Britain.

III. GLOBAL POSITIONING SYSTEM

A. INTRODUCTION

For thousands of years men have been navigating this planet by a variety of ingenious means. A navigational technique developed by the ancient Polynesians is the use of natural stars (Parkinson & Spilker, 1996). This method involved triangulating your position from the known location of the stars. After the development of radio technology, new methods of navigation were introduced. These methods included radio beacons, Vhf Omnidirectional Radios (VORs), and LOng-range RAdio Navigation (LORAN) (Parkinson & Spilker). Much like navigating by the stars, radio navigation involved finding one's relative position in reference to a known position - in this case a radio transmitter. Both of these systems had significant drawbacks. To navigate using the stars, the weather had to be clear enough to see them. To navigate using radio beacons, the user had to be within line-of-sight of the transmitter which limited the range of operations. With the introduction of artificial satellites, both of these limitations seemed to have been solved.

Artificial satellites made possible a revolution in navigation. Instead of using angular measurements to

natural stars, a plan was developed by a small group in the Department of Defense to use ranging measurements from artificial stars (satellites) to greatly improve accuracy and virtually eliminate the problems of line-of-sight caused by natural and man-made obstructions. This led to the birth of the Global Positioning System, more commonly referred to as GPS.

The Global Positioning System was developed by the US Department of Defense for military users. It took over two decades and ten billion dollars to deploy the twenty-seven satellite system (Pace et al., 1995). The benefits of GPS are enormous. GPS provides highly accurate navigation and positioning for a variety of military equipment, including aircraft, ships, land vehicles, and most recently precision-guided munitions (PGMs). US forces have come to rely heavily on uninterrupted access to GPS as it has emerged as an integral component of almost every military system. A recent RAND report states that, "The US military is moving toward high reliance on GPS, and force structure decisions are being made that assume GPS availability"(Pace et al., 1995, p. xvii). For example, Congress has ordered that any aircraft, ship, armored vehicle, or indirect-fire weapon not equipped with GPS after the year 2000 will not be funded (Pace et al.). These developments carry obvious benefits,

but there are risks as well. The more reliant we become on a continuous GPS signal, the more vulnerable we are when that signal is disrupted. The military, furthermore, is not the only organization that is increasingly relying on GPS coverage.

Although GPS was developed to meet military needs, the commercial uses of GPS are expanding at an ever-increasing rate. GPS is used extensively in civil aviation and some organizations are pushing to have GPS as the single source navigation system for all civil aviation due to its low cost and versatility (Corrigan et al., 1999). Besides basic land and marine navigation, other civilian uses of GPS include mapping and surveying, construction, wildlife management, resource exploration, space operations, and law enforcement (Aerospace Corporation, 1999). The hot new items in cars are moving map displays and vehicle tracking options - all made possible by GPS technology. One area that is rapidly expanding is the use of GPS time data. Accurate timing is essential for the seamless routing of "information packets" in communications systems and computer networks. GPS is the most cost-effective and efficient method to deliver precision time "stamps" so essential to the increased data rates of modern communication networks (Pace et al., 1995).

B. BACKGROUND

The theory behind GPS is quite simple - triangulation from known satellite positions -- but the actual working of the system is much more complex. To understand the strengths and weaknesses of the GPS system, a more detailed examination of how and why the system works is required.

1. GPS Segments

The Global Positioning System consists of three major segments: Space, Control, and User. All three segments are critical to the proper functioning of the entire system.

The first element of the GPS system, the Space segment, consists of the actual satellites orbiting the earth. Currently, there are twenty-four operational satellites and three spares that provide continuous worldwide coverage (Pace et al., 1995). The satellites are arranged in three circular rings spaced evenly about the equator at an orbital altitude of 10,980 NM. Providing a minimum of six satellites in view at any time (and a maximum of eleven), the system is robust in that it could tolerate occasional satellite outages (Parkinson & Spilker, 1996). To get accurate position and time information, only four satellites are required. Additionally, the current configuration of three orbital rings allows three spares to replace any single failure in the whole system (Parkinson & Spilker).

The satellites, once launched, are not autonomous. They require periodic updates to ensure accurate data is provided to the user.

The second element of GPS is the Control segment. The control segment consists of the Operational Control Center and five monitor stations. The Operational Control Center is located at Schriever Air Force Base (formerly Falcon AFB) in Colorado Springs, Colorado. The five monitor stations are located at Hawaii, Colorado Springs, Ascension Island, Diego Garcia, and at Kwajalein Island in the West Pacific. The Control Segment is responsible for the following functions: maintaining the proper position of the satellites through small commanded maneuvers, performing adjustments and corrections to the satellite clocks and payload, tracking the satellites and uploading the required navigation data, and finally relocating satellites in the event of a satellite's failure (Parkinson & Spilker, 1996). Without monitoring from the control segment, the accuracy of the system cannot be maintained.

The User Segment is the last major element of GPS. It consists of GPS receivers and the user community. GPS receivers convert the signals from the satellites to position, velocity, and time estimates. Four satellites are necessary to accurately compute the four dimensions of X, Y,

Z (position) and Time (Dana, 1999). Generally, the receivers track more satellite signals than the four required. By tracking more than four satellites, position accuracy can be maintained as satellites move out of view of the receiver. This is especially important for airborne GPS receivers due to the relative high velocities in all three dimensions. On the other hand, land and marine GPS navigation can operate for limited periods on only two or three satellites (Parkinson & Spilker, 1996).

The Space, Control, and User segments of GPS cover the hardware of the system, but just as important -- especially if we are to consider the vulnerability of GPS -- is the actual signal that the satellites transmit. The following is a brief overview of the GPS signal, how it is controlled, and the difference in the signal provided for military operations and the signal provided for civilian use.

2. GPS Signal

To better understand GPS and how the signal can be vulnerable to unintentional or intentional interference, we need to examine the intricacies of the signal transmitted by the satellites. GPS satellites transmit two distinct signals. The first is the Coarse Acquisition or C/A code. Designed for use by nonmilitary users, the C/A code provides the Standard Positioning Service (SPS). The C/A code is

less accurate, easier to acquire, and easier to jam (Pace et al., 1995). The code signal and navigation message for SPS is carried on the L1 frequency (1575.42 MHz). The C/A code modulates the L1 carrier signal and spreads the signal over a 1 MHz bandwidth spectrum (Dana, 1999). The accuracy of the SPS signal is intentionally downgraded by the Department of Defense by the use of Selective Availability (S/A). With selective availability, the SPS signal will provide at least 100 meter horizontal accuracy, 140 meter vertical accuracy, and 340 nanosecond time accuracy (Parkinson & Spilker, 1996).

The second signal provided by the satellite to the user is the Precision or P-code. Designed for authorized military users only, the P-code provides the Precise Positioning Service (PPS) (Pace et al., 1995). PPS data is transmitted on the L1 frequency and an additional L2 frequency. The L2 frequency (1227.60 MHz), the P-code, is provided to measure time delays between the two signals providing greater position accuracy. In addition, the L2 signal is spread over a 10 MHz bandwidth spectrum (Dana, 1999). The PPS accuracy is as low as 22 meter horizontal accuracy, 27.7 meter vertical accuracy, and a 100 nanosecond time accuracy - a significant improvement over the SPS code with Selective Availability activated (US Naval Observatory,

1998). The P-code is more difficult to acquire, therefore, current military GPS receivers first track the less accurate C/A code and then transfer to the P-code (Pace et al., 1995).

The PPS code can be denied to unauthorized users by cryptography. The DoD has the ability to encrypt a segment of the P-code. This technique is called anti-spoofing (AS) (Pace et al., 1995). Spoofing is a type of jamming in which a false signal is transmitted in an attempt to duplicate the real signal. The goal is for the receiver to track the false signal, thereby inducing errors in the navigation solution. When anti-spoofing is activated, the normal P-code is replaced by the Y-code, commonly referred to as the P(Y)-code (US Naval Observatory, 1998). To realize the accuracy of the Precise Positioning Service in the anti-spoofing mode of operation, the user requires a classified AS module for each receiver channel and the proper cryptographic keys (Dana, 1999).

This brief overview of how GPS works only scratches the surface of a highly technical and complex system. Much more about the signal characteristics of GPS will be discussed when GPS vulnerability is examined later in this chapter.

C. GPS AS A CRITICAL TECHNOLOGY

GPS is rapidly becoming the standard means of navigation for almost every military platform. It would be hard to find a soldier, sailor, or airman who does not have at least some experience with GPS. The enormous growth of GPS started in the Gulf War. The featureless terrain and the long and rapid movements made navigating in the desert extremely difficult. It quickly became apparent that GPS provided a distinct advantage. With GPS, Coalition forces were able to navigate at night and in adverse conditions when the Iraqi troops who lived there could not. The demand for GPS receivers was so great that more than 9000 commercial receivers were purchased and used in the Gulf by everyone from foot soldiers to aircrews (Aerospace Corporation, 1999). SOF units were some of the first and only units to have a GPS capability at the start of the war. The 20th Special Operations Squadron, flying the MH-53J PAVELOW helicopter, started the air war when members led a flight of Apache helicopters across the desert at night to destroy selected Iraqi air defense sites and blow a hole in the Iraqi air defense system for the Coalition Air Force. The MH-53Js got the job because they were the only helicopters in the theater with the navigation system (GPS included) capable of the precise navigation and exact timing

the mission demanded. SOF has always been a leader in the development and use of new technologies and GPS is no exception. The question now remains whether GPS is a "critical technology" for SOF in the manner in which this concept has been previously defined. To answer this question, the three criteria of dependence, vulnerability, and substitutability are examined below.

1. Dependence

It is obvious that GPS usage by SOF, as well as the entire Department of Defense, has risen dramatically in the last decade, but has SOF become dependent on GPS to accomplish its mission? The level of dependency on any current technology is difficult to quantify. Operators are often unwilling to admit their success relies on a single piece of gear and this is generally true. Mission success is seldom determined by the availability of a single technology, but mission effectiveness and level of risk can be impacted by a single technology. Realizing that dependency is not clearly quantifiable, dependency on GPS must be established subjectively. In order to accomplish this task, I have reviewed the navigation equipment carried by various SOF units and how the equipment is used in the field. The following information was compiled from informal interviews with SOF operators. The data do not reflect how

GPS would be used for each of the wide range of missions various SOF units may be required to perform, but rather provides a broad snapshot of GPS use.

A few general trends are readily apparent when examining GPS use by SOF units. It is obvious that terrain and speed of maneuver have a significant impact on the level of dependency on GPS. The more featureless the terrain - such as desert, open water, dense foliage - the greater the reliance on alternate forms of navigation. Also, the faster the movement and the greater the distance covered the more opportunity there is for error, especially when allowable 'time on target' tolerances are plus or minus thirty seconds, or less. A review of the equipment carried by various SOF units will provide insight into the level of dependence on GPS.

SOF aviation is one of the primary users of GPS technologies. All SOF aviation assets currently have on-board GPS units. On some airframes, such as the two versions of the H-6 'Little Bird', the only on board navigation systems are GPS and LORAN (Jackson, 1998). All SOF MC-130 aircraft and most of the SOF helicopters have GPS integrated with inertial navigation systems (INS). The GPS provides nearly continuous updates to the INS to provide the

best navigation solution. In other words, the GPS is always on and providing vital input to the navigation systems.

Ground units also carry GPS units on a regular basis. Special Forces (SF) teams carry GPS units on all mission activities. The number of GPS units carried varies based on mission, equipment load, and team preference. An SFODA can carry as many as three GPS units for navigational assistance. The majority of SF units are using the Rockwell AN/PSN-11 Precision Lightweight Global Positioning System (PLGR). GPS units are also mounted on the various vehicles used by SF teams.

The US Air Force Special Tactics Squadrons (STS) and the Navy SEALs also carry the PLGR for navigation. Much like SF, the number of GPS units carried depends on team size and mission tasking, but GPS units are always carried - usually more than one per team. Multiple units are regularly carried to provide redundancy should a unit fail. Most SEAL units are also equipped with the Miniature Underwater Global Positioning System Receiver (MUGR) manufactured by the Trimble Corporation. The MUGR weights less than twenty ounces and is designed to operate to a water depth of 33 feet (Williamson, 1998).

The different SOF units rely on GPS to varying degrees. This is evident by the type of training conducted and the

mission environment. Of all the SOF components surveyed, US Army Special Forces appear to be the least dependent on GPS technology for overall mission accomplishment. This fact reflects a combination of mission environment and training. As previously stated, the level of reliance varies significantly with the type of terrain and method of movement. Walking patrols tend to use the GPS only as a backup at irregular intervals, whereas vehicle mounted patrols tend to have a much greater reliance.

SF units do train without GPS availability on a recurring basis. All initial training is accomplished without the aid of GPS and each member is required to demonstrate his basic land navigation[1] skills during recertification exercises that are conducted each year.

SEALs also conduct initial navigation training without the use of GPS and some recurring training is conducted using only basic navigation skills, but on a much less structured basis. There is no formal requirement such as yearly recertification. The maritime environment, due to the lack of navigation reference points, lends itself to greater reliance on GPS as a continuous source of

---

[1] Basic land navigation involves navigating using only a map, compass, stopwatch, etc. No outside signal is sent or received by the user to aid in position determination.

navigation. On land, by contrast, GPS is used more as a position verification tool. The same is true for STS units, although STS appears to train even less without GPS availability than other SOF units.

Lastly, SOF aviation assets use GPS on a near continuous basis. GPS is fully integrated into the navigation systems of the aircraft and provide continuous input. Training without GPS is normally only conducted on training flights involving upgrades to a higher crew qualification or on evaluation flights.

Although the various aspects of SOF do train to varying degrees without the aid of GPS navigation, no known joint special operations exercise has been conducted that required all participants to conduct operations without the aid of GPS navigation. It is readily apparent that training without GPS is only done unilaterally at the unit or service component level, if conducted at all. Additionally, the longer SOF successfully uses GPS and the more comfortable operators become using and trusting GPS, the greater the impact will be should the GPS signal be lost.

2. Vulnerability

The Global Positioning System satellites may be orbiting at 11,000 miles above the earth and out of reach of most weapons, but there is a weakness of GPS that is

potentially vulnerable to enemy exploitation. The most vulnerable aspect of GPS is the navigation and timing signals coming from the satellite to the receivers on the ground or in the air. Like any other radio signal, GPS signals have the potential of being disrupted. These disruptions can be unintentional or intentional and can seriously degrade the quality of signal reaching the GPS receivers. GPS signals are more susceptible to interference than ground based navigation systems due to the relatively weak signal strength of GPS. The satellites provide a signal whose power level is -160 dBW (160 decibels below a watt) - a mere whisper when compared to most radio transmissions (Alterman, 1995).

a) Unintentional Interference

Unintentional interference of GPS navigation signals can come from a variety of sources. Layers of the atmosphere, especially the ionosphere and troposphere, can interfere with GPS signals and produce errors in receiver accuracy (Parkinson & Spilker, 1996). Additionally, commercial very high frequency (VHF) radio transmitters can drown-out the weak GPS signals and cause loss of navigational data (Corrigan et al., 1999). Lastly, certain television transmissions can cause similar difficulties.

Television stations often use very high power transmitters compared to GPS signal strength. Three television channels, channels 23, 66, and 67, all have harmonics that fall within the L1 band and their power levels are much stronger than that of the GPS signal (Corrigan et al.). The interference caused by VHF and television transmitters is generally intermittent and localized, therefore, the threat to GPS navigation is not significant. However, the fact that GPS can be disrupted by common signals does give us some insight into the possible effectiveness of the intentional disruption of GPS signals by an adversary intent on degrading US military capability.

b) Intentional Interference

> It is well know that the GPS signal is very weak, and, assuming a standard GPS receiver, a small level of noise in the GPS band can disrupt reception over tens or even hundreds of miles. (Corrigan et al., 1999)

Considering the relative weakness of the GPS signal, noise jamming - a more pervasive threat than spoofing - can be very effective. "This approach [noise jamming] attempts to overwhelm a GPS receiver (by brute force) with radio noise" (Pace et al., 1995, p.49). Either wide-band jamming or narrow-band jamming can be employed.

Wide-band jamming is much more effective, especially against military users, because jammer noise can be spread across the entire bandwidth of the P-code making the jamming difficult to counter (Pace et al., 1995). Jamming effectiveness depends on jamming power, range to receiver, and receiver characteristics.

To analyze the possible threat of GPS jamming, The Johns Hopkins University Applied Physics Laboratory in its *GPS Risk Assessment Study* (1999) developed a model to compare the estimated cost and size of a jammer vis-à-vis jammer power. Most of the parts required to build an effective jammer are readily available. An inexpensive frequency source, solid state transmitter, power supply, and onmi-directional antenna are all easily obtained. Only the frequency source is not readily available and must be specifically ordered (Corrigan et al.). Table 3.1, taken directly from the report, shows the estimated cost, weight, and volume of jammers at varying power levels. A 100W jammer designed to operate for a full day would only cost slightly over $400 and be the size of a small suitcase. The effect of such a small and inexpensive jammer is illustrated in Figure 3.1, also from the Johns Hopkins University's report. The shaded area of Figure 3.1 shows the area of

disruption of GPS C/A code signals at various flight altitudes caused by a 100W jammer. Depending on the altitude, a 100-w jammer alone can disrupt signals up to 210 miles away.

Power (W)	Operating Time					
	1 Hour			1 Day		
	Cost ($)	Weight (lb)	Volume (cu. in.)	Cost ($)	Weight (lb)	Volume (cu. in.)
10	50	1	50	60	11	250
100	300	3	500	409	112	2500
1000	3000	10	5000	4090	1100	25000

Table 3.1 GPS Jammer Characteristics From Ref. Corrigan et al., 1999, p. 5-6.

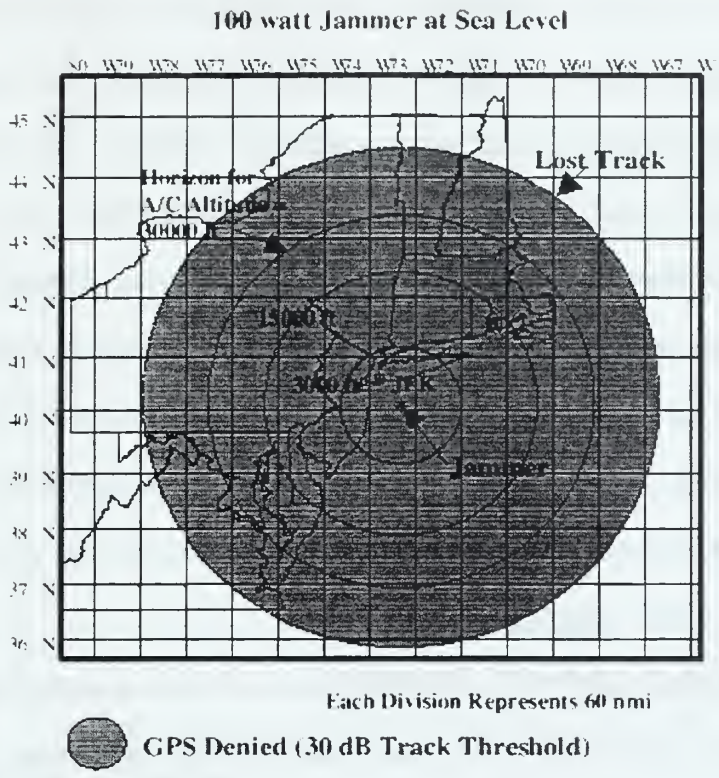

Figure 3.1 Outage Area Caused by a 100-W Jammer From Ref. Corrigan et al., 1999, p. 5-7.

There is more to the GPS jamming threat than just numbers and electronic theory. A portable GPS jammer is already on the market. Aviaconversia, a Russian electronics firm, displayed a GPS jammer at Moscow Air '97. According to *Aviation Week and Space Technology* (Sept, 1997), "the 4W jammer will interfere with civil and military frequencies out to a range of 200km (108 mi.)" (Nordwall, p.56). The jammer can be powered by batteries or 230 volts d.c. and weights only 18-26 lb. The next generation jammer is

expected to be 50% smaller and lighter. Aviaconversia claims to have several potential customers in the Middle East (Nordwall, 1997). The Russians are not the only ones developing this technology.

The Naval Warfare Center, China Lake, CA., has also developed a prototype GPS jammer. Twenty devices have been built in a variety of shapes - some as small as a Coke can. According to W. Mark Henderson, an electronic systems engineer from China Lake, the devices could be produced for as little as $250 (Nordwall, 1998).

The threat of jamming and the proliferation of jamming technology are not the end to GPS. Antenna design, receiver design, and increased signal strength are all techniques to mitigate the effects of jamming. There is already one method that decreases the threat of jamming - the use of receivers that are capable of receiving and encrypting the P(Y) code. Figure 3.2, taken from an article by Stanley Alterman (1995) in the *Journal of Electronic Defense*, clearly illustrates the effectiveness of using the P(Y) code and antenna design techniques. By examining the chart, we see that just a "1W jammer located 60 km away (line-of-sight) can prevent a well-designed GPS receiver using C/A-code from acquiring satellites" (p. 54). In contrast, a well-designed military receiver locked on to the

P(Y) code requires a 100 W jammer just 20 km away to disrupt the receiver (Alterman). Figure 3.2 also shows the advantages of antenna designs on jamming effectiveness. One type of adaptive antenna is the controlled radiation pattern antenna (CRPA). CRPA provides 20 to 30-dB jamming/signal rejection. A special nulling concept currently being developed can provide up to 50-dB jamming/ signal rejection (Alterman).

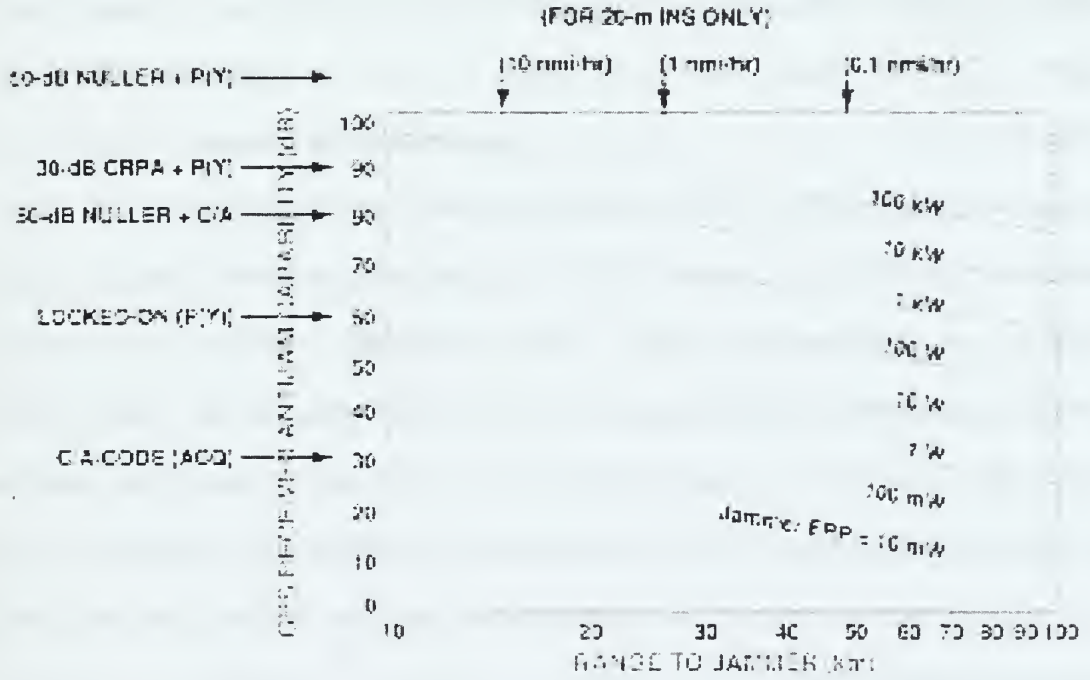

Figure 3.2 GPS Calculations From Ref. Alterman, 1995, p. 54.

GPS signals are vulnerable and becoming more vulnerable as companies such as Aviaconversia and others

develop cheaper and smaller jammers. As we have just seen, these current jammers can be defeated, but is SOF effectively using these techniques to minimize their exposure to intentional interference of the GPS signals? The following paragraphs hope to answer this question.

As previously noted, GPS vulnerability can be reduced through the proper use of encryption which permits use of the P(Y) code which not only increases accuracy, but is harder to jam once the P(Y) code is acquired. By sampling SF, STS, SEAL, and SOF aviation units, I have found that all the units surveyed have access to and use GPS units designed for military use, therefore, have the ability to receive the P(Y) code. There are individuals who carry commercial GPS units as part of their personal gear, but I found no indication that the commercial units were being used as a primary navigation aid; they are only carried for personal use in an emergency or survival situation. Although SOF units have access to military GPS units capable of encryption, are the operators taking advantage of this added capability?

Overall, SOF units are taking advantage of the added capability of encryption to receive the P(Y) code. Most of the operators interviewed stated that the units used in the field are usually keyed. Although it appears that

the GPS units are generally keyed, there is no indication that this is required in accordance with standard operating procedures or regulations. In addition, the operators are not fully aware of the importance of obtaining and maintaining the P-code during operations. Most operators were aware of increased accuracy, but most were not aware of the increased anti-jam capabilities that the P-code provided. By not realizing the full advantage of the encrypted GPS signal, less emphasis may be placed on proper encryption, possibly undermining the mission should jamming become a factor.

3. Substitutability

As mentioned at the beginning of this chapter, man has been successfully navigating the globe thousands of years before the advent of GPS. This being true, it would appear that GPS is easily substituted by using older, tried and true navigation techniques. However, it is not so easy. The modern battlefield environment demands a level of precision and timeliness that is unmatched by any other period in modern history. Modern military operations can require timing to the second and position accuracy to the meter. At the moment, only GPS can provide this capability. In addition, SOF units do not have the luxury of picking the environment in which they operate. Desert operations and

extended maritime operations are just two environments that can exceed the capabilities of even the best trained operators using no navigation aids besides map and compass techniques.

Currently few navigational techniques can provide the accuracy of GPS navigation for the majority of SOF units. For most SOF land and sea based units, GPS is the only realistic alternative currently available that can provide the required accuracy in all environments. There are alternatives to GPS, but accuracy is sacrificed and complexity is usually increased. Ground-based navigation aids and inertial navigation systems are two alternatives, but each has significant limitations for many applications.

Many SOF aviation assets, and some SEAL boat units have the capability to use some of the ground based navigation systems previously mentioned such as VORs, TACANs or LORAN. Although many of the assets are equipped to navigate using these systems, it is unrealistic to assume that these systems will be available in the conflict's area of operation. If an enemy can jam GPS signals, they can jam ground based navigation systems. In addition, these systems lack the accuracy required and are limited by line-of-sight. Another possible substitute, especially for aviation assets, is inertial navigation.

Inertial navigation systems (INS) use internal gyros to measure accelerations on the X, Y, and Z axes. By tracking the accelerations in all three axes, a computer can calculate the relative position of the units from a known starting point (Farrell, 1999).

INS has been in use in SOF aircraft for decades. All models of the MC-130 have navigation systems that include INS. In addition, the MH-53J, the MH-47D/E, and the MH-60K use INS as an integral part of their navigation solution. Technology innovations have allowed INS units to achieve higher accuracy at lower costs, but INS does have some limitations. First, in order for an INS to provide accurate navigational data, a precise starting position must be entered into the INS computer. Currently, GPS is the best source for an accurate starting position. Otherwise, the starting location must be a presurveyed site with known coordinates.

Second, inertial navigation is not as accurate as GPS. "A pure INS integrates differential equations containing inertial measurements to provide a navigation solution. As a result, small errors in the measurements can lead to large velocity and position errors if allowed to integrate without correction for long time periods" (Farrell, 1999, p.1). I do not want to imply that INS is not an effective navigation

aid. Integrated with GPS, INS can provide a highly accurate navigation solution when GPS is intermittent or unavailable in certain geographical areas. Unfortunately, INS is not currently feasible for all SOF platforms, especially ground units. SOF Technology Development is exploring personal inertial navigation systems, but they are still in the developmental stage (SOF Posture Statement, 1998). Even with the technological innovation in INS development, the size, weight, and power requirements of current INS systems prevent their use by individual ground units (Farrell, 1999).

D. SUMMARY

The Global Positioning System is integrated into every aspect of military operations. This integration has been mandated by Congress and embraced by all the services.

After a review of SOF navigation equipment and interviews with SOF operators, I can only conclude that SOF is moving toward dependence on GPS systems for position orientation. This trend will increase as the culture changes and GPS is accepted as a primary navigation aid. Currently, emphasis is still placed on basic land navigation, but the trend is more and more toward dependence on GPS.

GPS is vulnerable! GPS relies on a weak UHF radio signal from a satellite located thousands of miles above the earth's surface. Unintentional and intentional interference is a concern wherever GPS is used. Although there has been no evidence that any nation has intentionally interfered with GPS signals to gain an advantage in time of conflict, it does not mean that GPS jamming is not possible. The capability to jam GPS signals is available to any buyer and will only get better, especially if a market develops that supports development in the industry.

Lastly, there are some substitutes to GPS navigation, but those substitutes cannot provide the position and timing accuracy in all the environments in which SOF must operate. Technological innovation may enable internal navigation systems to approach the accuracy of GPS, even for the individual soldier, but that could be a long way in the future.

GPS passes the test of *criticality*. GPS is a vulnerable technology that SOF is dependent on, yet there are no current substitutes that provide the same capability.

IV. SATELLITE COMMUNICATIONS

A. INTRODUCTION

Communications is vital to the successful conduct of military operations on the modern battlefield. The modern warfighting environment demands that forces operate seamlessly in an ever expanding and multi-dimensional battlefield. Only through timely and accurate information can forces committed simultaneously to widely separated objectives achieve the synergy necessary to shape the battlespace and rapidly destroy or neutralize enemy centers of gravity. Information is rapidly becoming a strategic resource that soldiers depend on to execute their endless variety of missions (Griffith, 1998).

There is no question that this trend will continue well into the coming decades. The operational concepts of Joint Vision 2010 include dominant maneuver and precision engagement. Both concepts rely heavily on seamless communications between dissimilar platforms over large distances. Currently, the only way to effectively communicate in this matter is via satellites.

Satellites permit direct communications on the battlefield between widely dispersed units. No longer do units have to maintain line-of-sight relay stations to

ensure stable communications. Nor do they have to rely on terrestrial networks[2] - networks that are usually insufficient or nonexistent in many parts of the world.

The development of satellite communications predated the development of the GPS system but followed a similar course. The objectives of communication research have been to achieve ever-increasing ranges and capabilities while at the same time reducing costs. Satellite communications were the direct result of this research. The Second World War prompted the development of two technologies that would eventually lead to the era of satellite communications. These technologies were missiles and microwaves. The combinations of these technologies enabled satellite communications to become a reality (Maral & Bousquet, 1998).

The space era started in 1957 when the Soviets launched the first artificial satellite (Sputnik). Only eight years later, the first commercial geostationary satellite, INTELSAT I, went into service and started a revolution in worldwide communications that continues today (Maral & Bousquet, 1998).

In just three short decades, all aspects of the military have fully embraced satellite communications as an

---

[2] Terrestrial systems use cable, including fiber optics, to achieve connectivity between stations.

integral part of tactical and strategic operations. Operations DESERT SHIELD and DESERT STORM ushered in the widespread use of satellite communications that continues today. Over 1500 SATCOM terminals were eventually deployed to the theater to provide the critical communication links between dispersed forces in the absence of any communications infrastructure across much of the area of operations. Of the over 1500 terminals used, more than 75% were single-channel man-portable military and commercial units (Dunmeyer, 1997). Even with the military and commercial systems, the operation lacked sufficient capacity to support all the requirements for joint and combined operations.

The following background discussion will provide a brief overview of military satellite communications and some principles behind their operation. Although the discussion addresses some technical subject matter, it is only presented to provide a better understanding of satellite communications and not a detailed analysis of the technical aspects of satellite operations.

B. BACKGROUND

The military satellite communications (MILSATCOM) architecture is comprised of four segments (Pike, 1997). The first segment is the ultra high frequency (UHF) satellites that provide the bulk of the communications capability to SOF ground, sea, and air forces (Pike). This segment consists of FLTSATCOM, AFSATCOM, LEASAT, and UHF FollowOn (UFO) systems - all designed to support tactical mobile forces. The super high frequency (SHF) Defense Satellite Communications System (DSCS) is the second segment of MILSATCOM. DSCS supports high volume data transmission for command and control functions. Satisfying the majority of DoD's medium and high data-rate communications, DSCS is much less mobile than the UHF systems due to the size of the user terminals and antennas. The third segment is the Military Strategic/Tactical Relay (MILSTAR) system. MILSTAR is designed to support strategic level command and control, but will also provide additional capabilities for tactical users. MILSTAR operates in the extremely high frequency (EHF) range (Pike, 1997). The fourth and final segment consists of commercial communication satellites. Commercial satellites are used to augment the DoD's MILSATCOM capabilities when demands require additional assets (Pike, 1997). INMARSAT is just one example of DoD's use of

commercial satellite systems to expand communication capabilities.

The focus of this research is the first segment of the MILSATCOM architecture - tactical UHF satellite communications. There are two reasons why UHF SATCOM is being tested as a 'critical technology'. UHF SATCOM is used much more than any other type of satellite communications for connectivity of tactical units. UHF SATCOM provides the backbone of long-range communications for SEALS, Special Forces, and SOF aviation assets. Second, UHF SATCOM, due to its signal characteristics, is the most vulnerable to enemy countermeasures. In addition, tactical UHF satellite terminals have proliferated throughout all the military services, consequently, user requirements for UHF SATCOM are greater than the resources available (Griffith, 1997).

The following sections describe how satellite communication systems work. A basic understanding of SATCOM is required to understand how it can be vulnerable and how that vulnerability can be reduced.

1. Satellite Operation and Components

Communication satellites are nothing more than a relay station for radio signals placed on a very high 'hill'. In its simplest form, satellite communications involves the

transmission of an RF signal from an earth-based station[3] to the satellite (the uplink), followed by the retransmission from the satellite of another RF signal (the downlink) to a different earth-based station (Leonard, 1999). The primary components of a communication satellite are the receiver and receive antenna, transmitter and transmit antenna, and a power source. The capabilities and efficiency of a satellite depend greatly on the frequency range, power source and antenna design.

Band	Range (Ghz)	Principal Use	Feature
UHF	0.3 - 3	Military Commercial	Manpack Terminals Crowded Spectrum
SHF	3 - 30	Military Commercial	Primarily Vehicular Terminals Greater Capacity
EHF	30 - 300	Military Emerging	Compact Equiment Survivable

Table 4.1 Communications Satellite Frequency Bands. From Ref. Griffith, 1998, p. 101.

2. Frequency Bands

Military satellite communications operate in three frequency bands - UHF, SHF, and EHF. The UHF frequency band is used primarily for mobile and tactical satellite

[3] An earth-based station is any terrestrial satellite communications terminal including fixed or mobile ground terminals, maritime terminals, and terminals aboard aviation assets.

services. SHF satellite communications are more capable, yet require larger terminals. EHF band communications are currently being developed by both civilian and military agencies that will provide even greater capacity, yet offer the mobility of UHF systems.

An advantage of higher frequencies is greater bandwidth. The greater the bandwidth, the greater the information carrying capacity of the satellite channel. For example, operating in the 4 - 6GHz frequency range provides a bandwidth of 500 MHz, but operating in the 20 - 30 GHz range provides bandwidths of 3500 MHz - a sevenfold increase (Griffith, 1998). Greater bandwidths not only provide faster data transfer, but they also provide improved jam resistance. Additionally, larger bandwidths can be divided into smaller segments enabling more users to use the same channel. This process can involve numerous control techniques such as Frequency Division Multiple Access (FDMA), Code Division Multiple Access (CDMA), or Demand Assigned Multiple Access (DAMA) (Griffith, 1998).

3. Orbits

Communication satellites can be deployed into one of four types of orbit depending on the desired coverage, the nature of the satellite's mission, and the performance of the launchers. The four orbits are geosynchronous

(equatorial) orbits, elliptical orbits, low earth orbits (LEO), and medium earth orbits (MEO) (Maral, 1998). Each orbit type has unique advantages.

The geosynchronous orbit is by the far the most popular. There are currently more than 200 satellites in geosynchronous orbit. The area above the North American continent and the Atlantic Ocean is especially congested (Maral, 1998). The orbit is called geosynchronous because the "satellite thus appears as a fixed point in the sky and ensures continuous operation as a radio relay in real time for the area of visibility of the satellite" (Maral, p. 3). Flying over the equator at an altitude of 35,786 km (23,300 miles) and at a speed equal to the earth's rotation, a geostationary satellite can cover 42% of the earth's surface. Only three satellites in geosynchronous orbit can cover the entire earth except for the polar regions (Leonard, 1999).

The second type of orbit used for communications satellites is the elliptical orbit. Elliptical orbits are inclined at an angle of approximately 64 degrees with respect to the equatorial plane (Maral, 1998). An elliptical orbit allows the satellite to cover the regions of higher latitudes for extended periods as it proceeds to its apogee. Three phased satellites on different orbits can

provide continuous coverage of a selected polar region. For example, the Russians use this type of orbit to ensure coverage to even the most northern reaches of their territory (Maral).

The last two orbits are the low earth orbit (LEO) and the medium earth orbit (MEO). The LEO has an altitude of 830 km and the orbit inclination varies based upon coverage requirements. It would take a constellation of approximately thirty satellites to provide worldwide coverage. The MEO has an altitude of approximately 10,000 km. Only 10 to 15 satellites in a MEO are required to provide the same worldwide coverage (Maral). Although many more LEO satellites and MEO satellites are required to maintain continuous coverage, the reduced power requirements (due to the reduced distance between the ground station and the satellite) enable the satellite to be much smaller and less expensive and also reduces the power required by the transmitting earth-station. In addition, it is much easier to launch a satellite into a LOE or MOE than a geosynchronous orbit.

The previous discussion is presented only as a primer and only includes the most basic information required to begin to understand the complex nature of satellite communications.

C. SATELLITE COMMUNICATIONS AS A CRITICAL TECHNOLOGY

> The contingency [communication] planner has many options for C4ISR support, although satellite communications remain the most important means for connectivity. This is not expected to change anytime soon. (Griffith, 1998, p. 87)

Reliable long-range communications are especially important for SOF operations. Special operations forces are often tasked to conduct a variety of missions far from established communication networks. The often politically sensitive nature of SOF operations requires reliable communications to ensure connectivity between the operators and the National Command Authority. Although SOF may operate under the premise of 'centralized control and decentralized execution', it is unrealistic to think that the NCA will not demand an ability to monitor the operation. In addition, special operations forces can be tasked to provide 'eyes on the target' when other means of surveillance are unavailable. Special Reconnaissance (SR) is a principal mission for SOF forces. Successful SR demands the ability to communicate from any location and at any time - a defining capability of satellite communications. As previously mentioned, UHF SATCOM is the only segment of the MILSATCOM system that will be examined

as a 'critical technology' based upon the criteria of dependence, vulnerability, and substitutability.

1. Dependence

> Global mission requirements, greater information transfer requirements, and rapidly increasing C4I technological advances combine to place enormous demands on SOF communications. (Griffith, 1997, p. 2-2)

UHF SATCOM is used extensively by special operations ground units and aviation units to provide essential connectivity. Much like GPS usage, SATCOM usage is difficult to accurately quantify due to the same reasons mentioned in the previous chapter. To determine the level of dependence on UHF SATCOM the same methods are used that were used to establish GPS dependence. These methods include a review of the long-range communications equipment carried by SOF forces and informal interviews with SOF operators from SEAL, SF, and STS ground units and Army and Air Force aviation units. All SOF units require long-range communications capability, but how the units employ this capability varies a great deal.

Army Special Forces are normally required to carry four long-range capable radios, though of course this can change based on mission requirements. The four radios include UHF SATCOM primary and backup and HF primary and backup. There

is considerable emphasis by SF Command to ensure all SFODAs are proficient using HF radios. SF Groups often require each deployed team to make at least two contacts per week via HF to ensure connectivity. Even with the emphasis on HF, UHF SATCOM still accounts for a large majority of communications when channels are available. This is mainly due to the greater ease of use and better capabilities of SATCOM versus HF radios. Similar conditions are found in other ground units.

Air Force Special Tactics personnel use and train with HF much less than does Army SF. Frequently, HF radios are not even carried by the teams, requiring a complete dependence on SATCOM for all long-range communications. Considering that successful HF radio connectivity is often dependent on user training and skill - it was even called an 'art' by one operator - units not regularly communicating via HF will degrade that capability. There is no question that STS is able to communicate via HF radios, but the less comfortable the teams are with HF the less likely they will be to use HF when SATCOM is degraded.

Navy SEALs also rely on UHF SATCOM for long-range communications. Much like SF and STS, SEALS carry both HF and UHF SATCOM radios, but the vast majority of the teams' long-range communications are carried via SATCOM channels.

All SOF aviation assets currently have UHF SATCOM capability and rely on it much more than on HF. Until recent modifications added a HF capability, versions of the H-6 'Little Bird' only had a UHF SATCOM (Jackson, 1998). The importance of UHF SATCOM was clearly demonstrated when SOF forces deployed to Haiti for Operation UPHOLD DEMOCRACY.

Part of the contingent that deployed to Haiti as part of Operation UPHOLD DEMOCRACY was the 3rd Special Forces Group (SFG). One of the 3rd Group's responsibilities was to provide security and assistance to the people throughout the countryside. This required numerous SFODA teams to establish operations in the remote regions of Haiti. After years of internal strife, Haitian infrastructure was devastated. No telephone service existed throughout the island nation and few communities even had electricity. In addition, the mountainous countryside made line-of-sight communications virtually impossible. Satellite Communications became the only reliable means for the teams to send and receive information (Briefing by Colonel Mark Boyatt, August 1999). Colonel Mark Boyatt, the Army Special Operations Task Force Commander in Haiti, relied on daily UHF SATCOM broadcast to relay critical force protection information to the widely dispersed SFODAs. Without UHF SATCOM, the level of coordination between the SF teams would

have been significantly reduced, thereby reducing overall mission effectiveness.

2. Vulnerability

As previously mentioned, UHF SATCOM is the workhouse of the MILSATCOM system and accounts for the bulk of the tactical capability provided to dispersed and highly mobile SOF units. Unfortunately, UHF SATCOM is the most vulnerable to detection, interception, and jamming (Griffith, 1998). UHF SATCOM vulnerability is based not only on signal characteristics, but also on satellite antenna design and coverage.[4]

Antenna design can have a significant impact on the vulnerability of a SATCOM RF signal. There are two basic antenna designs. The first is a spot beam - a focused RF pattern sent only to a limited geographical area. The second antenna pattern is the Earth Coverage (EC) beam. Having a dispersed antenna pattern, the EC beam covers a large geographical area. A jammer located anywhere in the coverage area of an EC beam can induce noise on the uplink signal used by the satellite. Since the UHF transponder merely retransmits the same signal on the downlink with the

---

[4] Although satellites can be vulnerable to other types of threats such as physical destruction of the satellite or the ground control stations, only electronic vulnerabilities are discussed for the purpose of this thesis.

same jammer induced noise, the retransmitted noise then affects the entire area of the EC beam -- effectively jamming the whole coverage area of the satellite in the jammed frequency range.

The characteristics of the UHF signal make it more vulnerable to jamming than the higher frequency bands. UHF, with its small bandwidth, cannot effectively filter out jammer induced noise without losing total or partial signal integrity. The threat of electronic jamming is real and has been developed over decades by the former Soviet Union.

The capability to jam UHF signals is widespread. In the early 1970's the Soviets developed a whole new type of warfare - Radio Electronic Combat (REC). Radio Electronic Combat was integrated into all aspects of Soviet military doctrine and became an integral part of the operations of all the military services (Chizum, 1985). The legacy of the Soviets' emphasis on REC is a mature capability that has proliferated throughout the world. A review of classified and unclassified sources reveals a plethora of jammers capable of disrupting signals in the UHF spectrum.

The final aspect that makes UHF SATCOM vulnerable is the sheer number of users trying to gain access to a limited number of channels. "Tactical satellite terminal equipment has proliferated within all the military services. As a

consequence, user requirements for UHF SATCOM are normally greater than the resources available to satisfy them" (Griffith, 1998). The previous quote from the *C4ISR Handbook for Contingency Planning* clarifies the problem. Self-imposed 'jamming' through signal saturation may be just as problematic as enemy jamming. Every operator interviewed cited problems with SATCOM channel availability. There is no guarantee that SOF units will get priority - possibly forcing units to employ means other than UHF SATCOM for long-range communications.

3. Substitutability

Although UHF SATCOM is presently the backbone of the MILSATCOM system's tactical communication capability, it is not the only method of long-range communication for small, dispersed units. To evaluate the substitutability of UHF SATCOM, the following paragraphs will examine current long-range communication capabilities, particularly by HF Radio, and future systems that are in development that could replace UHF SATCOM.

Before the advent of satellite communications, HF (High Frequency) radio was the primary transmission means for over-the-horizon communications (Griffith, 1998). Although the military role of HF radio has diminished significantly

over the last decade, it is still a viable, yet less capable alternative.

HF radio differs greatly from satellite communications to achieve long range communications. HF radio works by bouncing the RF signal off the ionized layers of the earth's upper atmosphere. Layers of the ionosphere act as mirrors to reflect the radio waves beyond the horizon in a somewhat predictable manner (Griffith). Although HF systems are less expensive than satellite networks and recent technological advances have made HF radio more reliable, HF radio still has significant drawbacks when used in a military environment.

HF radio can support only a relatively small bandwidth. Generally useful for only voice transmissions, HF radio can accommodate limited data transfer, but only at a 300- 600 baud rate (Griffith). HF radio is also vulnerable to enemy direction finding and jamming. Since HF relies on bouncing the RF signal off the atmosphere, weather patterns, sunspots, man-made electronic noise, and other phenomena can cause severe signal disruption or atmospheric blackout (Griffith). Lastly, "HF is the most extensively used international frequency band, a fact that complicates the frequency acquisition process"(p. 73). Not only do military users have to compete among themselves for available

frequencies, but they must compete with civilian users as well.

HF communications are also less suitable in a tactical environment where mobility and speed are required. HF radios often require much more time to setup and teardown than UHF SATCOM systems. HF transmissions generally require long antennas that must be stretched out above the ground before transmissions can be made or received. This increases a unit's signature and reduces its mobility.

HF radio remains a low-capacity alternative to satellite communications for some applications, but HF radio is not a substitute for the high band-width requirements of special operations forces in our highly communications intensive environment.

One system that is rapidly being developed that could replace UHF SATCOM for the tactical user is MILSTAR. MILSTAR operates in the EHF portion of the electromagnetic spectrum making it a much more capable and survivable system.

First, the antenna design of the MILSTAR satellite mitigates jammer effectiveness. The MILSTAR satellite, transmitting in the EHF spectrum, has the capacity to use multiple spot beams. Unlike the earth coverage antenna of the UHF SATCOM systems, if a jammer is located within the

spot beam, it affects only the area of the spot beam, allowing the remaining coverage to be used normally.

Another feature of the EHF signal is the multiple access control techniques employed by MILSTAR. One such technique that is quite jam-resistant is Code Division Multiple Access (CDMA). CDMA is "a dynamic multiple access technique where the total transponder bandwidth employs a separate and distinct code for each user to access a traffic channel at any instant in time. This technique is also called spread spectrum (Griffith, 1998, p. 104). Without the proper user code, the satellite transponder will not accept the signal, therefore, it filters out the noise from the jammer.

The higher frequencies, once again, allow much higher bandwidths. The high bandwidths give EHF satellite communications added jam-resistance. With such a wide bandwidth, noise can be filtered out without losing the original signal. The very wide EHF bandwidth allows it to operate below the noise level induced by a RF jammer, making it almost immune to induced noise.

Lastly, due to the highly directional antennas used with EHF TACSAT communications radios, there is a low probability of intercept and direction finding, unlike UHF SATCOM antennas (Field Manual 24-11, 1990). The Rockwell

Corporation has developed an EHF man-portable terminal to work with the MILSTAR system, but it weights almost thirty pounds and is much bulkier than current portable UHF SATCOM systems (Williamson,1998). Unfortunately, tactical MILSTAR systems are not yet in use by tactical units.

Other commercial satellite systems offer promise as substitutes for UHF SATCOM for the tactical user. Companies such as Iridium, Teledesic, Globalstar, and Celestri are developing systems to provide worldwide coverage using small, mostly hand-held units (Griffith, 1998). All of the above systems use LOE or MEO satellite constellations. For example, Iridium uses sixty-six satellites in low earth orbit to maintain continuous coverage. Due to the large number of satellites and the corresponding small coverage area of each satellite, these systems will make it difficult to effectively jam the transmissions.

D. SUMMARY

SATCOM is the only way to provide reliable, global communications in a timely manner. Other means of communications have inherent limitations. High frequency radio lacks the reliability and the capacity required for military operations. Line of sight radios have neither the range required nor the ability to operate in all

topographical areas. Finally, landlines are often not available, take a long time to install, and are highly vulnerable to disruption. Satellite communications have become an integral part of DoD activities including special operations. After examining the factors that define *critical* technologies for SOF, it appears that UHF SATCOM is a *critical* technology, but it may not remain so for long.

Special operations assets are dependent on UHF SATCOM for reliable long-range communications. Every ground unit and every aviation platform has a UHF SATCOM capability and UHF SATCOM carries the vast majority of long-range transmissions. Additionally, the primary substitute for UHF SATCOM, HF, is being used less and less.

UHF SATCOM is vulnerable! The signal characteristics and antenna design make UHF SATCOM the most vulnerable military satellite system presently deployed. Countries such as the former Soviet Union spent decades developing and maturing systems designed to disrupt the UHF portion of the electromagnetic spectrum. It would be unwise to think that this knowledge has not proliferated to other potential adversaries. The last area of vulnerability for UHF SATCOM is channel saturation. UHF SATCOM channel availability is not expanding as rapidly as user demand. Too many users

trying to use too few channels can be just as disruptive as enemy jamming.

Currently, there may be no substitutes for UHF SATCOM for the individual SOF operator, except the less capable HF radio. However, this is changing fast. With the advances in telecommunications UHF SATCOM, with its inherent limitations, will be replaced by much more capable and secure systems such as man-portable MILSTAR terminals or other commercial systems that are more mobile and less susceptible to disruption.

Special operations tactical units are dependent upon UHF SATCOM for long-range communications and the system is vulnerable to disruption by an adversary and from our own overuse. What will soon change is the substitutability of UHF SATCOM. Other more secure and reliable systems are being deployed that will have the capacity to meet the increasing demand for satellite communications on the modern battlefield.

V. SUMMARY/ FINDINGS/ RECOMMENDATONS

> When war is transformed, it can be transformed for all belligerents. A national lead is possible, indeed it is a fact for the United States today, but a permanent national lead is not certain. Moreover, even if (improbably) the United States alone can enjoy the benefits of space age information warfare for the next several decades, enemies will be motivated to find ways to restrict the domain of information led military advantage. (Gray, 1996)

A. SUMMARY

Technology and continued technological advancement are essential to modern warfighting and will continue to be so as advancements in navigation, communication, mobility, logistics, and intelligence continue at an ever increasing pace. Superior technology has provided the United States military, including special operations forces, with significant advantages over our adversaries in recent conflicts, but the United States cannot and must not become comfortable with the advantages we currently maintain. Additionally, the United States must guard against *relying* on technologies that are *vulnerable* to enemy actions. This thesis proposed a model that can be used by all levels - strategic, operational, and tactical - to evaluate our use

of technologies to determine if they are *critical* to successful mission accomplishment.

The previous case studies were used to illustrate the concept of *criticality* presented in the first chapter. For a technology to be considered critical it must first be evaluated against three factors - dependence, vulnerability, and substitutability. Dependence is satisfied if the technology is required to perform the mission or the absence of a given technology will significantly decrease expected mission effectiveness. Second, for a technology to be considered vulnerable it must be reasonably susceptible to enemy exploitation, degradation, or destruction. Lastly, the technology cannot have any readily available substitutes that can replace it without loss of mission effectiveness or increased risk to the users. None of these variables are easily quantifiable. All require subjective judgements on a case-by-case basis to determine if the criteria are met and in what circumstances.

The purpose of this thesis is not to discount the relative advantages technological innovation provides SOF on the battlefield. Nor does this thesis promote a change in course away from technology as a means to gain an advantage. By developing the model and applying it to a historical case and two current cases, I hope to encourage special

operations forces at all levels to look beyond the immediate advantage of a technology. War is a dynamic, interactive process in which both sides are trying to out-maneuver, outwit, and overcome their adversary's forces over time. A technological advantage or capability enjoyed at the onset of the conflict may not be available at the end. Presently, no adversary is capable of challenging the United States directly, therefore, we can only assume that our adversaries will use asymmetric strategies to avoid our strengths and exploit our weaknesses (Edwards, 1997). The model developed in this thesis provides a framework from which to evaluate current and future technologies to determine if a technology can be exploited and turned into a weakness for the US.

B. FINDINGS

Radar, GPS, and UHF SATCOM are by no means the only cases of *critical* technologies. They are only used to illustrate how technologies can and should be evaluated, not only once deployed, but also during the development and procurement stages. The current examples used in this thesis and the method in which they were evaluated are at the tactical level of employment only, but the *critical* technology model developed in this thesis can be used for every level of combat analysis - strategic, operational, or

tactical. Other technologies that could fall into these categories and may be considered *critical* might include those supporting the Global Command and Control System (GCCS), stealth technology, tactical and strategic mobility, and any commercial-off-the -shelf (COTS) items that can be acquired, evaluated, and possibly exploited by any one of our adversaries.

Probably the biggest question is: why should we be worried? No country has been able to challenge the US technologically and there are very few countries in the world that have demonstrated the potential to do so. No nation has conducted widespread jamming of the GPS signal in an effort to disrupt our military activities. The same can be said about UHF SATCOM. Disrupting or degrading GPS or UHF SATCOM certainly can be done, but it would take an adversary with sufficient resources and sophistication to do so in an effective and sustained manner. Furthermore, we have substitute technologies or techniques in many cases that will allow our forces to operate in some capacity. The answer, of course, is that just because an enemy has not struck at a *critical* technology does not mean one will not. If the enemy does strike, will we be ready for the consequences? The next section takes this point to the

extreme, but in doing so it illustrates our potential technological vulnerabilities.

1. Electro-magnetic Pulse

Electromagnetic pulse (EMP) and the effects of EMP have been recognized for over three decades. The first evidence of EMP effects occurred when the US detonated an atomic device above Johnson Island in July 1962. Just seconds after the blast, the Hawaiian Islands, over 800 miles to the northeast, experienced severe electrical problems including tripped burglar alarms, tripped circuit breakers, and extensive power outages (McGrath, 1992). EMP is a real and dangerous phenomenon.

Electromagnetic pulse is a high voltage burst of energy, much like a lightning bolt. The pulse lasts for just a fraction of a second but can render unprotected electronics useless, especially modern electronics. As circuits get smaller and smaller and required voltages are reduced, the possible effects of EMP are even greater. EMP can cause a variety of adverse effects. In the case of digital logic circuits, these effects can include transient, resettable, or permanent damage. The damage can be caused directly by the collected EMP resulting in system failure, or EMP can trigger internal power sources to respond in unintended ways that can also cause system failure (U.S.

House of Representatives, 1997). If electronic equipment is turned off, it is less likely to be damaged. If the equipment is turned on, the rapid increase in current will cause every semiconductor to go into overdrive and overheat (Edwards, 1997).

There are two general types of EMP - nuclear and non-nuclear. The first and most common type is electromagnetic pulse produced from the detonation of a nuclear device. The physics of how the pulse is produced from the nuclear reaction is beyond the scope of this study, but a few factors concerning bomb delivery are relevant. The amount of EMP experienced by electronic systems depends on weapon yield, location of burst, altitude of burst, and type of weapon (U.S. House of Representatives, 1997). Basically, anything within line of sight of the blast can be affected. For example, a high yield weapon detonated 250 miles above the center of the continental United States would affect electronics from coast to coast (U.S. House of Representatives). The likelihood of an adversary detonating a nuclear device over the US is, admittedly, small. Not only does a state have to develop a warhead; it must also have a delivery vehicle capable of achieving sufficient altitude and distance to maximize effectiveness. The more likely scenario could involve detonating a nuclear device

over US forces prior to, or instead of, a conventional attack (Edwards, 1997). This scenario would require a much smaller warhead and a much less sophisticated delivery platform. Due to our high reliance on the microchip in almost every platform and piece of communication gear, much of our military capability would be devastated, yet not one building would be destroyed, nor would any US soldier be killed. Conversely, an enemy well prepared for an EMP event can protect its equipment and significantly reduce the effects. Will the U.S. then have enough justification to retaliate in kind if the adversary's "clean" use of a nuclear weapon did not directly injure a single U.S. soldier (Edwards, 1997)? This is the dilemma of nuclear EMP.

Non-nuclear electromagnetic pulse should also concern US forces. The physics behind nuclear and non-nuclear EMP differ, but the results are similar although different in scale. Non-nuclear EMP weapons use complex explosives to generate a powerful, yet short lived, electrical field (Kopp, 1997). The footprint of non-nuclear EMP devices is considerably smaller than that of a nuclear device. Non-nuclear devices may affect areas of tens of meters to several hundreds of meters in radius (Kopp). Possible targets are tactical operations centers, communications nodes, or Corps/ Wing level headquarters. Non-nuclear EMP

weapons are not only technically feasible, but also relatively inexpensive to build when compared to the costs associated with a nuclear weapons program. Due to the relatively isolated effects of non-nuclear EMP weapons, they are not currently able to devastate a theater force. However, they do not have to. Even temporary disruption of our electronics by EMP may be enough to change the course of the battle.

EMP effects can be mitigated. Electronic devices can be hardened against EMP. If EMP hardening is built in from the start, the costs of EMP hardening can be as little as 1-5% of total system costs (U.S. House of Representatives, 1997). If done after the fact, the costs are significantly higher. Some military systems are hardened against EMP, but considering that 95% of all military communications go through commercial channels, the expense of hardening all COTS systems would be unreasonable.

Considering the effects of Electro-magnetic pulse, we must assume that any unhardened piece of electronics is potentially vulnerable. It is also clear that all U.S. forces are becoming increasingly reliant on advanced technologies in almost every aspect of military operations - during peacetime and in war. Not all technologies will be considered *critical*, but many will.

C. RECOMMENDATIONS

This research would not be complete without some recommendations concerning critical technologies. No technology should be "critical" to mission accomplishment, but due to the wide variety and complexity of special operations missions there may be no way to avoid dependence on some vulnerable technologies. There are two methods to mitigate the risks posed by critical technologies. One method is to develop technological fixes and redundant systems. The second method is to develop doctrinal offsets.

Of the three factors that define critical technologies, substitutability can be addressed through advanced technological development to provide redundancy for all systems. SOF is active in pursuing this course. By considering only the two recent cases presented in this thesis, we can see that SOF has an ongoing research and development effort in many areas of long-range communications. Advances in HF radio are making these radios more capable and easier to use. In addition, satellite systems using a different frequency bands and employing varying orbital configurations are being developed to supplement UHF SATCOM and reduce vulnerabilities. By having so many redundant systems, we can possibly take UHF SATCOM off the critical list.

Advances in precision navigation methods are not likely to replace GPS in the near future. Here too, USSOCOM is actively exploring alternates to GPS, such as INS units for individual soldiers, but much more has to be done in this field to make it possible. Technology cannot be the only fix to the problem. As I have argued before, we must realize that a motivated and creative adversary can develop countermeasures to our new technologies. The United States cannot assume that the technological advantage we enjoy today will last forever.

The other method for addressing the criticality issue is through doctrinal changes and training. Joint doctrine should address the loss of significant capabilities. Tactics, techniques, and procedures should be developed to ensure continued operations if communication, navigation, computing, or mobility capabilities are lost or significantly degraded. Obviously, operations will not continue as before and a decrease in effectiveness should be expected. Yet, with proper planning, operations should not cease.

Coinciding closely with doctrine is a training program to test SOF's capabilities in a degraded environment. Once doctrine is developed, it must be put into practice through training exercises that simulate the loss of a *critical*

technology. As I previously stated, I have found no evidence that SOF has been forced to operate without GPS during any major exercise. Doctrine cannot be written and training exercises cannot be conducted to prepare for the loss of every technology applicable to special operations. It will be up to individual commanders to decide which technologies are most critical based on mission requirements and the operating environment -- only then can contingency plans and training programs be developed to deal with the technology loss.

The United States can never assume a continuous technological advantage. Worldwide technology proliferation and the rapid advancement of computing capability allows any nation to obtain significant technical capabilities at relatively low cost and possibly faster than our own acquisition system allows. SOF must continue to innovate and diversify- as it has in the past - in order to remain a competitive force. However, the innovation and diversification cannot only be in technology. They must also be in doctrine and training to ensure continued relevance in an unpredictable world.

LIST OF REFERENCES

Aerospace Corporation. GPS primer [Online]. Available: hppt://www.aero.org/publications/GPSPRIMER/. (1999, July 6).

Alterman, S. (1995, September). GPS dependence: A fragile vision for US battlefield dominance. Journal of Electronic Defense, 18, 52-56.

Buderi, R. (1996). The invention that changed the world. New York: Simon and Schuster.

Chizum, D. (1985). Soviet radioelectronic combat. Boulder Co.: Westview Press.

Clark, R. (1966). Battle for Britain. New York: Franklin Watts.

Corrigan, T., Hartranft, J., Levy, L., Parker, K., Pritchett,J., Pue, A., Pullen, S., & Thompson, T. (1999, January). GPS risk assessment study: Final report. Maryland: The Johns Hopkins University Applied Physics Laboratory.

Dana, P. (1999, January 2). Global positioning system overview[Online].Available:hppt://www.utexas.edu/depts/grg/gcraft/notes/gps/gps.html (1999, July 21).

Department of Defense. United States Special Operations Forces: Posture Statement 1988. (Washington, D.C.: Dept. of Defense (OSD-SO/LIC), 1988).

Dunmyer, J. (1997, September 25) The ultimate high ground! Space support to the army: Lessons from operations DESERT SHIELD and DESERT STORM [Online]. Available: hppt://call.army.mil/call/newsltrs/91-3/chap4.htm (1999, October 11).

Edwards, S. (1997, Autumn). The threat of high altitude electromagnetic pulse to force XXI. National Security Studies Quarterly, 61-80.

Farrell, J. & Barth, M. (1999). The global positioning system and inertial navigation. New York: McGraw-Hill.

Fisher, D. (1988). A race on the edge of time: Radar - the decisive weapon of World War II. New York: McGraw-Hill.

Gray, C. (1996). The influence of space power upon history. Comparative Strategy, 15, 293-308.

Griffith, J., Lee, O., Pirog, T., Sielski, K., & Trahan, R. (1997, December). Contingency C4ISR Handbook for Integrated Planning Appendix K: U.S. Special Operations Command C4I Systems and Networks. Washington, D.C.: Dept. of Defense (ASD-C3I).

Griffith, J., Lee, O., Pirog, T., Sielski, K., & Trahan, R. (1998, August). Contingency C4ISR Handbook for Integrated Planning. Washington, D.C.: Dept. of Defense (ASD-C3I).

Holmes, R. (1988). The world atlas of warfare. New York: Viking Studio Books.

Jackson, P. (Ed.) (1998). Jane's all the world's aircraft. Alexandria, VA: Jane's Information Group, Inc.

Jefferson, P. (1989, July). National scene. Aerospace America, 13.

Kopp, C., (1996, November). An introduction to the technical and operational aspects of the electromagnetic bomb. Australia: Air Power Studies Center, Royal Australian Air Force.

Leonard, R. Satellite communications - a short course [Online]. Available: http://ctd.grc.nasa.gov/rleonard/regs1i.html. (1999, August 16).

Maral, G., & Bousquet, M. (1998). Satellite communications systems. New York: John Wiley & Sons.

McGrath, S., The electromagnetic pulse environment and its influence on tactical electronic and communications equipment, Master's Thesis, Naval Postgraduate School, Monterey, California, March 1992.

Mosley, L. (1977). The Battle of Britain. Chicago: Time-Life Books.

Nordwall, B. (1997, September 29). Filter center. Aviation Week and Space Technology, 149, 56.

Nordwall, B. (1998, November 23). 'Navwar' expands EW challenge. Aviation Week and Space Technology, 149,57-58.

Pace, S., Frost, G., Lachow, I., Frelinger, D., Fossum, D., Wassem, D., & Pinto, M.(1995). The global positioning system: Assessing national policies. Santa Monica, CA: RAND.

Parkinson, B., & Spilker, J. (Eds.). (1996). Global positioning system: Theory and applications. Vol 1. Washington DC: American Institute of Aeronautics and Astronautics, Inc.

Pike, J. (1997, March 9). Military space programs Online]. Available:http://www.fas.org/spp/military/program/com/overview.htm (1999, August 16).

Posen, B. (1984). The sources of military doctrine. Ithaca: Cornell University Press.

U.S. Army Field Manual 24-11. (1990, September 20). Tactical satellite communications. Headquarters: Department of the Army.

U.S. House of Representatives: Hearing before the Military Research and Development Subcommittee of the Committee on National Security, July 16, 1997. *Threat Posed by Electromagnetic Pulse (EMP) to U.S. Military Systems and Civil Infrastructure.* (Washington, D.C.: GPO, 1998).

U.S. Naval Observatory. (1998, December, 1). USNO NAVSTAR global positioning system [Online]. Available: hppt://tycho.usno.navy.mil/gpsinfo.html. (1999, July 21).

Walsh, E. (1997, August). Critical technologies survey defines new tactical bearing. Signal, 40-43.

Williamson, J. (Ed.). (1998). Jane's military communications. Alexandria, VA: Jane's Information Group, Inc.

INITIAL DISTRIBUTION LIST

1. Defense Technical Information Center 2
   8725 John J. Kingman Rd., STE 0944
   Ft. Belvoir, VA 22060-6218

2. Dudley Knox Library 2
   Naval Postgraduate School
   411 Dyer Rd.
   Monterey, CA 93943-5101

3. Professor Gordon McCormick 1
   Chairman, Special Operations Academic Group
   (Code CC/Mc)
   Naval Postgraduate School
   Monterey, CA 93943-5000

4. The Honorable Brian Sheridan 1
   Assistant Secretary of Defense for SO/LIC
   The Pentagon, RM 2E258
   Washington, D.C. 20301-2500

5. GEN Peter J. Schoomaker 1
   Commander in Chief
   US Special Operations Command
   MacDill AFB, FL 33608-6001

6. LTG William Tagney 1
   Commander
   US Army Special Operations Command
   Ft. Bragg, NC 28307-5000

7. MG Bryan D. Brown 1
   Commander
   Joint Special Operations Command
   Ft. Bragg, NC 28307-50008

8. RADM Eric T. Olson 1
   Commander
   Naval Special Warfare Command
   NAB Coronado
   San Diego, CA 92155

9. LT GEN Clay Bailey 1
Commander
Air Force Special Operations Command
Hurlburt Field, FL 32544

10. Jennifer Duncan 5
Special Operations Academic Group
Code (CC/Jd)
Naval Postgraduate School
Monterey, CA 93943-5000

11. Library 1
Army War College
Carlisle Barracks, PA 17013

12. Department of Military Strategy 1
National War College (NWMS)
Ft. Leslie J. McNair
Washington, DC 20319-6111

13. Library 1
Naval War College
Newport, RI 02840

14. US Army Command and General Staff College 1
ATTN: Library
Ft. Leavenworth, KS 66027-6900

15. Library 1
Air War College
Maxwell AFB, AL 36112-6428

16. US Military Academy 1
ATTN: Library
West Point, NY 10996

17. US Naval Academy 1
ATTN: Library
Annapolis, MD 21412

18. US Air Force Academy 1
ATTN: Library
Colorado Springs, CO 80840

19. Maraquat Memorial Library 1
US Army John F. Kennedy Special Warfare Center
Rm. C287, Bldg. 3915
Ft. Bragg, NC 28307-5000

20. US Special Operations Command 1
ATTN: Command Historian
McDill AFB, FL 33608-6001

21. Professor Anna Simons 1
Academic Associate, Special Operations Academic Group
(Code CC/Si)
Naval Postgraduate School
Monetery, CA 93943-5000

22. Major Lawrence McLaughlin 1
204 Gilchrist Road
Uniontown, PA 15401